

GeekBrains

Урок 2 Видео 3

Криптография

Режимы шифрования ECB и CBC

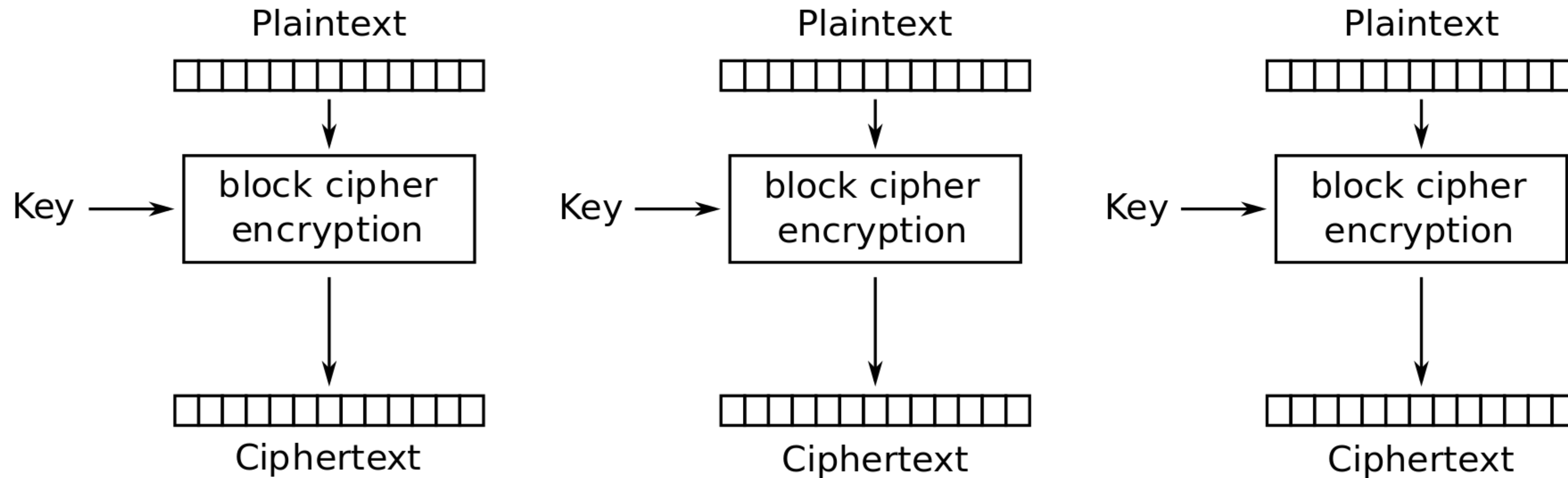
В этом видео

1. Назначение режимов шифрования
2. Режим шифрования ECB
3. Режим шифрования CBC
4. Определение режима шифрования

Что делать, когда размер открытого текста больше длины блока?

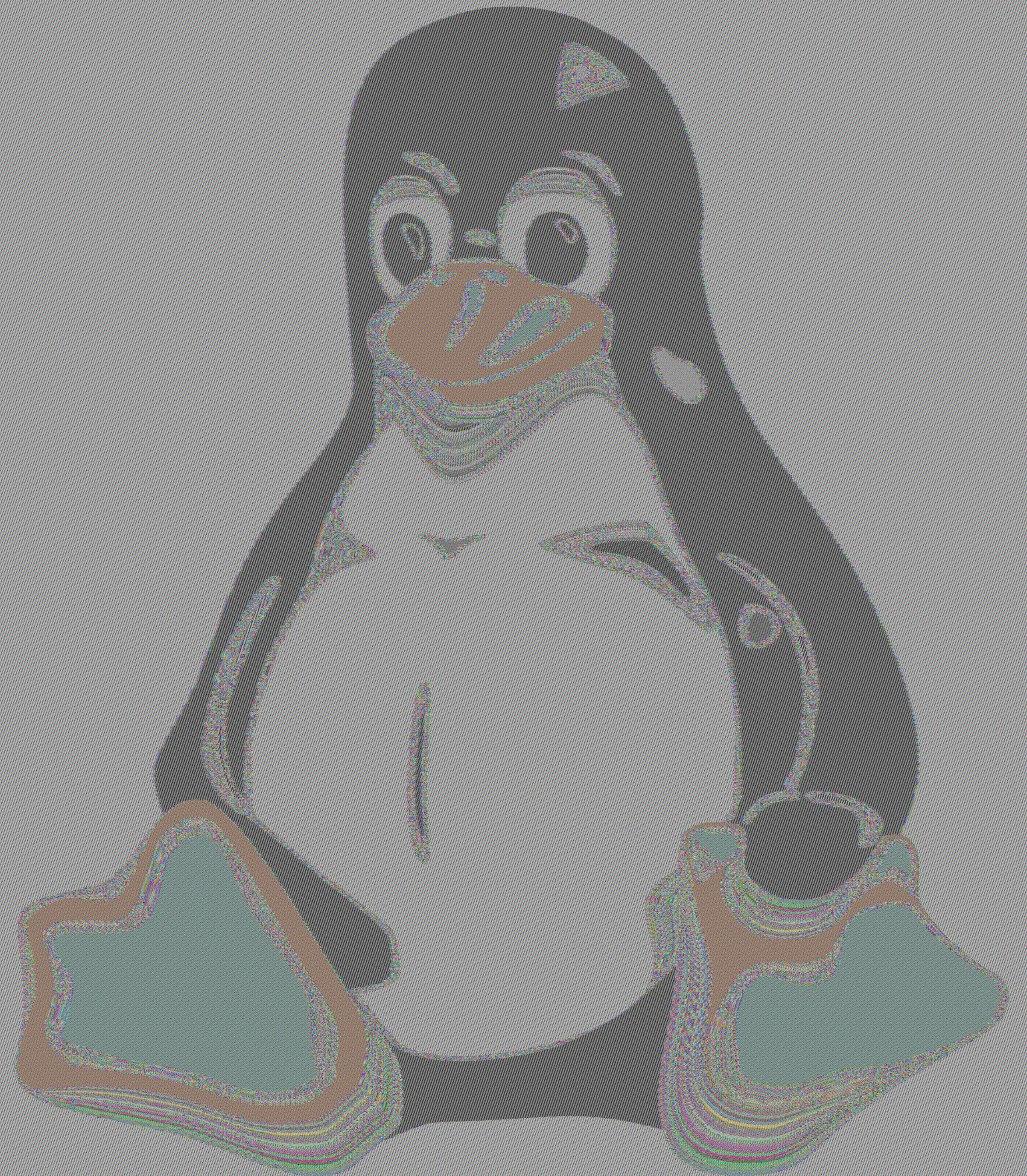


Режим шифрования ECB

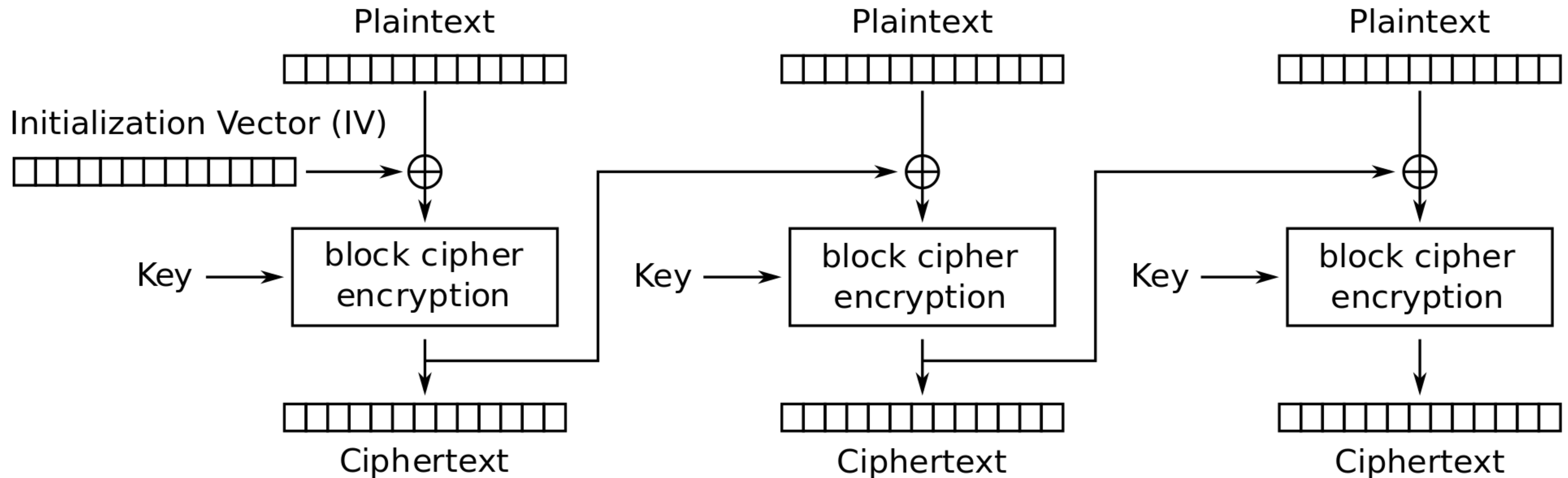


Картинка с пингвином

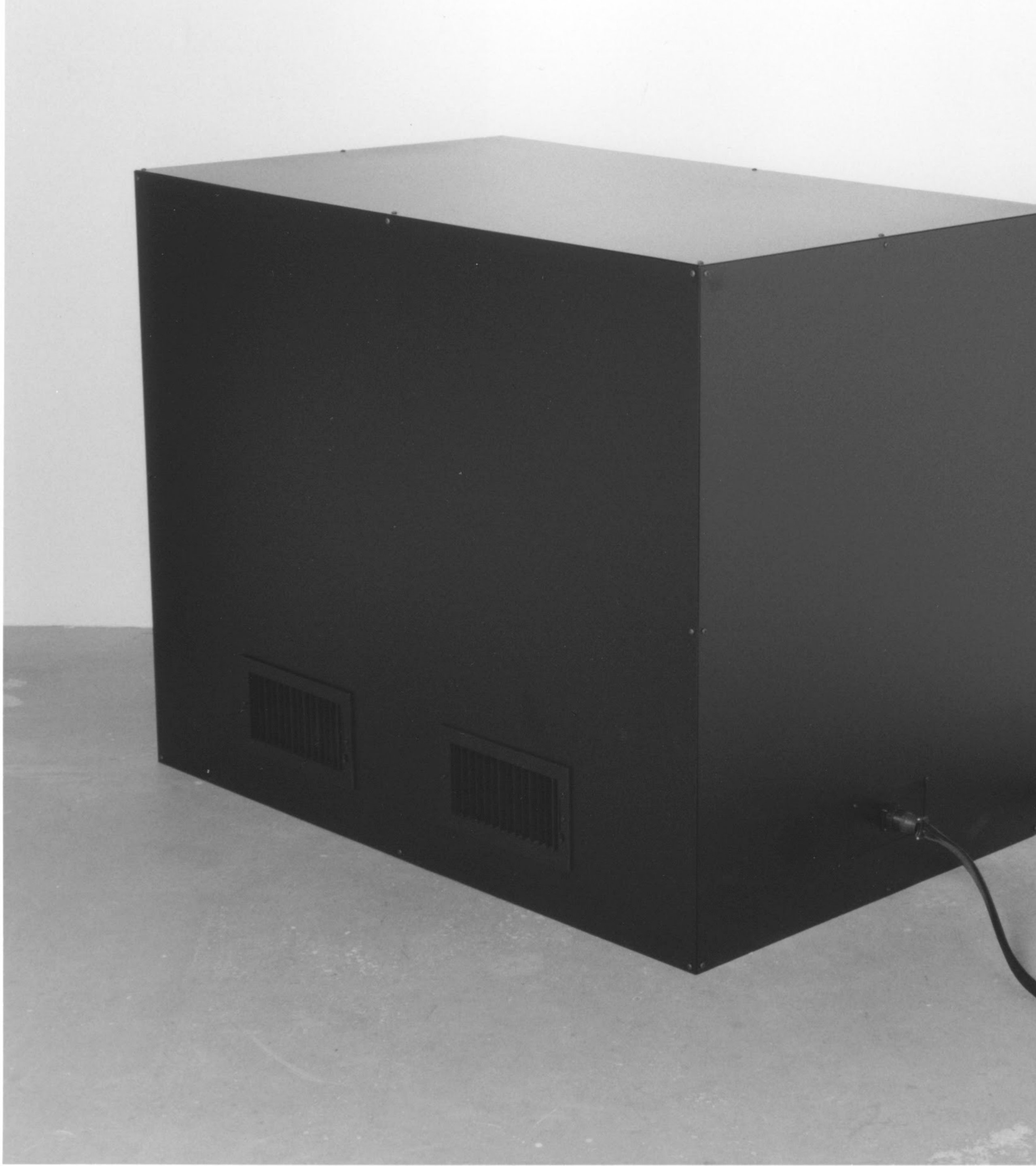
Главный недостаток режима шифрования ECB в том, что одинаковые блоки открытого текста дают одинаковые блоки шифротекста.



Режим шифрования CBC



Режим шифрования ECB
легко определить на больших объемах данных. Будут одинаковые блоки шифротекста.



Итоги

1. Узнали зачем нужны режимы шифрования
2. Режим шифрования ECB
3. Режим шифрования CBC
4. ECB/CBC detection oracle